PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-149022

(43)Date of publication of application : 06.06.1997

---

(51)Int.Cl. H04L 9/12

G11B 20/10

// G06F 1/00

G06F 12/14

---

(21)Application number : 07-304122 (71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 22.11.1995 (72)Inventor : OKABE YOSHIMASA

---

(54) DIGITAL DATA COMMUNICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To protect a copyright by inhibiting illegal use of digital data from a disk in a personal computer(PC) system including a disk driver and a reproduction board connecting to a CPU bus.

SOLUTION: A drive 1 (reproduction board 2) is provided with a random number generator 9 (12) of the same system, a random number as an initial value is transferred from the reproduction board 2 to the drive 1, a random number resulting from ciphering only head data of a sector from the drive 1 is returned and a time required for return has a limit. Then sector data including the head data are transferred and a discrimination device 16 discriminates the coincidence with the head data to inhibit the use of illegal data thereby preventing copy of data with the copyright on the PC.

LEGAL STATUS [Date of request for examination] 12.01.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3430752

[Date of registration] 23.05.2003

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] If initial value becomes settled to the 1st equipment and 2nd equipment which were connected through the circuit, respectively, the 1st random-number-generation equipment and the 2nd random-number-generation equipment which carry out sequential generating of the same random number of each other will be arranged after that. In advance of transmission of digital data, the random number generated by said 2nd random-number-generation equipment with the random number which was generated by the 1st random-number-generation equipment based on the initial value through said circuit as initial value in addition to said 1st random number generator The sector data which encipher the data of the peak value of the sector data which should be sent, and transmit and contain in said 2nd equipment continuously the data of said head section of the sector data which should be sent with the random number by which sequential generating is carried out with the 1st random-number-generation equipment Encipher, transmit to said 2nd equipment and it sets to said 2nd equipment. Decrypt the data of the head section with which the received above was enciphered with the random number by which sequential generating is carried out with said 2nd random-number-generation

equipment, and it memorizes to a register. Then, the enciphered sector data containing the data of said head section which received are decrypted with the random number of said 2nd random-number-generation equipment. The digital data communication mode characterized by intercepting the communication link between the 1st equipment and the 2nd equipment if it becomes the count at which coincidence with the head section data memorized to the head section data of the decrypted sector data and the aforementioned register was judged to be, and the count of an inequality was appointed beforehand.

[Claim 2] The random number which does not have a means by which the 2nd random-number-generation equipment inputs initial value, but was generated by said 2nd random-number-generation equipment After sending to said 1st random-number-generation equipment as initial value through said circuit The time amount taken to return the sector head section data encryption data enciphered with the random number generated by the 2nd equipment based on said initial value from the 1st equipment, The digital data communication mode according to claim 1 characterized by setting the tolerance of a difference with the time amount which generating of the random number used for said sector head section data encryption should take below to one half of the time amount which generating of said random number should take.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention is effective in duplicate prevention of the digital data with which especially copyright was set up about the digital data communication mode effective in prevention of unjust use of digital communication service.

[0002]

[Description of the Prior Art] Development of a record technique in recent years enabled it to record several G bytes of data on a small optical disk, and it became possible to carry out digital recording of the movie to the aforementioned optical disk with the technique of picture compression. The directions which reproduce the movie recorded on the aforementioned optical disk on the monitor of PC on the other hand by the development and spread of personal computers (it abbreviates to PC henceforth) appeared. With this use gestalt, the playback board which elongates and displays the drive equipment (it abbreviates to a drive henceforth) which reads an optical disk, and the image data by which compression record is carried out will be connected to the bus of

PC, and an image data transfer will be performed via this bus.

[0003] Since image quality does not deteriorate by the duplicate, a digital copy uses the function suitable for the duplicate and alteration of the data of PC, can copy image data to the hard disk drive (it abbreviates to HDD henceforth) and magnetic tape in PC, and can copy it to other PCs. However, since copyright is set to movie software and a duplicate and alteration are forbidden, it is necessary to make it the duplicate function which PC has not function effectively.

[0004] Since image data is transmitted through a bus when reproducing a movie with PC, the problem of duplicate prevention is concluded as the tapping prevention problem in a bus mold transmission line. Since it is difficult to detect and prevent wire tapping passive in a bus mold transmission line, it is common to perform cryptocommunication which cannot use the monitored data and which enciphers data like, and in order to perform cryptocommunication, a transmitting side and a receiving side need to share the secret information called a key.

[0005] The personal identification number method and cipher system which are also called a password system in that secret information is required are the same. JP,2-67067,A required the personal identification number, its personal identification number to which it was answered is inharmonious, or when there is no answerback into fixed time amount, it has proposed the method which refuses connection. In order to make small the probability for a right personal

identification number to be inputted by chance by trial-and-error, when JP,3-109850,A carries out fixed time amount progress from input initiation, it has proposed the method which inspects only once whether the right personal identification number of a right digit count is inputted. Although neither of the patents is adding detailed explanation to the setting approach of time amount, it is rational to think that it is set as the maximum of the time amount taken for an average user to input a personal identification number.

[0006] Drawing 2 is the block diagram of the conventional example, and, for a bus and 23, as for a playback board and 25, a drive and 24 are [21 / CPU and 22 / HDD and 26] bus monitor boards. As for actuation of this conventional example, CPU21 performs the input and updating of a key on drive 23 and the playback board 24 through a bus 22 according to software, using a key, drive 23 enciphers data, and is sent out, and the playback board 24 restores data using a key. Even if it is going to copy data to HDD25 and is going to transmit data to the playback board 24 from HDD25 later, unless the software which generates a key carries out the completely same actuation as last time, since this method cannot input into the playback board 24 the key used at the time of encryption, it cannot perform normal playback. However, if the key which said bus monitor board 26 incorporated also records in case a user connects the bus monitor board 26 to a bus, the bus monitor board 26 detects the writing of the key to the playback

board 24, a key incorporates and data record on HDD25, in case data will transmit from HDD 25 to a playback board 24 later, since the key used at the time of encryption is given by the playback board 24, normal playback can perform.

[0007]

[Problem(s) to be Solved by the Invention] Thus, in the system which reproduces the movie by the image and voice data which copyright has etc., a cryptographic key must be made secret with PC. Although the right to which PC user reproduces the image and voice data with which the movie on a disk etc. was recorded does not have, it has the just right which reproduces a movie etc. from the image and voice data which were dedicated to the disk.

[0008] Since a drive and a playback board need to share the same key, they need to input a key into a drive and a playback board using a certain means. Since there is no means to distinguish from the data by which the direct input was carried out from the drive in a playback board even when the key beforehand same at the time of shipment is inputted, the data which the drive outputted are once henceforth copied to HDD by the method which is not changed and it inputs into a playback board from HDD, a movie is reproduced like the usual playback. If the playback from HDD is possible, since other PCs which copied the data on HDD are reproducible, the method using the key of

immobilization is not effective as anti-copying.

[0009] Since exchange of the key between a drive and a playback board is performed within PC even when the method which updates a key is used during playback of a movie, acquisition of a key is possible under supervising the data flow in PC.

[0010] Therefore, in order to give effective anti-copying, it is not enough just to encipher data, and the communication mode to which a playback board can check that the data inputted into the playback board are the same as the data outputted from the drive to just before is required. Moreover, even when the secret about a code and a key is exposed to PC user as the worst case, a method with it very difficult [to deceive a playback board] is desirable.

[0011] Even when this invention solves the above-mentioned conventional trouble and the update procedure of a key is copied, the time amount which renewal of a key takes is inspected, a communication link is refused, and it aims at offering the digital data communication mode which realizes duplicate prevention of DIJITERU data.

[0012]

[Means for Solving the Problem] In order to solve said technical problem, the digital data communication mode of this invention If initial value becomes settled to the 1st equipment and 2nd equipment which were connected through the

circuit, respectively, the 1st random-number-generation equipment and the 2nd random-number-generation equipment which carry out sequential generating of the same random number of each other will be arranged after that. In advance of transmission of digital data, the random number generated by said 2nd random-number-generation equipment with the random number which was generated by the 1st random-number-generation equipment based on the initial value through said circuit as initial value in addition to said 1st random number generator The sector data which encipher the data of the peak value of the sector data which should be sent, and transmit and contain in said 2nd equipment continuously the data of said head section of the sector data which should be sent with the random number by which sequential generating is carried out with the 1st random-number-generation equipment Encipher, transmit to said 2nd equipment and it sets to said 2nd equipment. Decrypt the data of the head section with which the received above was enciphered with the random number by which sequential generating is carried out with said 2nd random-number-generation equipment, and it memorizes to a register. Then, the enciphered sector data containing the data of said head section which received are decrypted with the random number of said 2nd random-number-generation equipment. Coincidence with the head section data memorized to the head section data of the decrypted sector data and the aforementioned register is

judged, and if it becomes the count at which the count of an inequality was appointed beforehand, it will be characterized by intercepting the communication link between the 1st equipment and the 2nd equipment.

[0013] While judging the justification of data using some data which should be transmitted according to this invention, it is very difficult to obtain a cryptographic key required for playback of data unjustly, and it is effective in duplicate prevention.

[0014]

[Embodiment of the Invention] The digital communication method of this invention according to claim 1 If initial value becomes settled to the 1st equipment and 2nd equipment which were connected through the circuit, respectively, the 1st random-number-generation equipment and the 2nd random-number-generation equipment which carry out sequential generating of the same random number of each other will be arranged after that. In advance of transmission of digital data, the random number generated by said 2nd random-number-generation equipment with the random number which was generated by the 1st random-number-generation equipment based on the initial value through said circuit as initial value in addition to said 1st random number generator The sector data which encipher the data of the peak value of the sector data which should be sent, and transmit and contain in said 2nd

equipment continuously the data of said head section of the sector data which should be sent with the random number by which sequential generating is carried out with the 1st random-number-generation equipment Encipher, transmit to said 2nd equipment and it sets to said 2nd equipment. Decrypt the data of the head section with which the received above was enciphered with the random number by which sequential generating is carried out with said 2nd random-number-generation equipment, and it memorizes to a register. Then, the enciphered sector data containing the data of said head section which received are decrypted with the random number of said 2nd random-number-generation equipment. Coincidence with the head section data memorized to the head section data of the decrypted sector data and the aforementioned register is judged. The data used in order to be characterized by intercepting the communication link between the 1st equipment and the 2nd equipment and to judge the justification of data, if it becomes the count at which the count of an inequality was appointed beforehand It is some transmit data, and since it has judged for every sector data, the dependability of a judgment of just data can be increased.

[0015] Next, the digital data communication mode indicated by claim 2 The random number which does not have a means by which the 2nd random-number-generation equipment inputs initial value, but was generated by

said 2nd random-number-generation equipment After sending to said 1st random-number-generation equipment as initial value through said circuit The time amount taken to return the sector head section data encryption data enciphered with the random number generated by the 2nd equipment based on said initial value from the 1st equipment, It is characterized by setting below to one half of the time amount which generating of the random number used for said sector head section data encryption should take the tolerance obtained from a difference with the time amount which generating of a random number should take. Since decode of data cannot be performed normally and the 2nd random number generator does not have an initial value input means unless it prepares the random number generator which generates a random number in the high-speed clock frequency of 2/3 times or more for performing unjust reproduction Initial value is not forged, a safe random number generator is obtained, and playback of reliable data can be performed. Below, the gestalt of implementation of invention indicated by claim 1 of this invention and claim 2 is explained using drawing 1 . drawing 1 -- setting -- 1 -- a drive and 2 -- a playback board and 3 -- a bus, and 4 and 5 -- a bus interface, and 6 and 7 -- a clock circuit and 8 -- an encryption machine, and 9 and 12 -- the random number generator of 32-bit die length, and 10 -- a drive circuit and 11 -- a decoder and 13 -- for a counter and 16, as for a gate circuit and 18, a judgment machine and 17 are [a

timer and 14 / a register and 15 / an animation display circuit and 19] CPUs.

[0016] Actuation of each part of the image reproduction system constituted as mentioned above is explained. The drive 1 and the playback board 2 are connected to the bus 3. Bus interfaces 4 and 5 operate synchronizing with the clock which the clock circuits 6 and 7 generate, respectively. The clock circuits 6 and 7 operate on the same oscillation frequency. The bus interface 4 by the side of a drive has the encryption machine 8 and a random number generator 9. The encryption machine 8 enciphers the data inputted from the drive circuit 10 according to the random number which a random number generator 9 generates, and outputs them to a bus 3. By making into initial value the 32-bit random number inputted through the bus 3, a random number generator 9 carries out renewal of sequential of the random number outputted at 1 time of a rate, whenever it is read for every clock between the after [an input] 64 clocks of initial value and the encryption machine 8 is read once at the other period.

[0017] The bus interface 5 of a playback board has the decoder 11, the random number generator 12 and timer 13 which restore the enciphered data, a register 14, and a counter 15 and the judgment machine 16. A decoder 11 restores the encryption data written in from a bus 3 to the original data according to the random number which a random number generator 12 generates, and outputs them to a register 14, the judgment machine 16, and a gate circuit 17. Although

the period when the inhibiting signal has not come out of the gate circuit 17 from the judgment machine 16 outputs the input from a decoder 11 to the animation display circuit 18 as it is, the period out of which the inhibiting signal has come does not output data.

[0018] Data transfer from the drive 1 to the playback board 2 is blocked considering the fixed length called a sector as a unit. Said random number generator 12 is the thing of the same generating method as the random number generator 9 by the side of drive 1, and if both initial value is in agreement, sequential generating of the same random number will be henceforth carried out for both. Moreover, after outputting initial value, synchronizing with a random number generator 9, a random number generator 12 updates a random number at 1 time of a rate, whenever the period of an after [64 clocks of read-out of a random number] is written in a decoder 11 for every clock and data are written in once at the other period. However, since the random number generator 12 of the playback board 2 does not have a means to input the initial value of a random number unlike the random number generator 9 of drive 1, it is uncontrollable from the outside to generate a random number from specific initial value. A timer 13 measures time amount until the data with which the data encryption of the head section of the sector sent from a drive 1 side was carried out to the decoder 11 are written in, after a random number generator 12 reads

initial value. A register 14 memorizes the result to which the decoder 11 decoded 32 bits of data with which said head section was enciphered. What is necessary is just to decide not only 32 bits but 16 bits and at least 8 bits of numbers of bits of the data of the head section in consideration of the bus width of face of PC.

[0019] The judgment machine 16 outputs an inhibiting signal to a gate circuit 17 from the time of the random number of a random number generator 12 being read. A timer 13 measures time amount until a random number generator 12 sends out a random number and the data of the head section come on the contrary from a drive 1 side. Although time over is supervised, a counter 15 is counted up at the time of the inequality of the value of the time over of a timer 13, and the data of the head section, and the output of the inhibiting signal to a gate circuit 17 is suspended with the next clock at the time of a decoder 11 outputting the data of the head section when a counter value is less than eight When the value of a counter 15 is 8, the output of an inhibiting signal is continued as it is. The decode data of the head after read-out of a random number generator are not based on the value of a counter 15, and are not outputted to the animation display circuit 18, namely, the data of the head section of a sector are once used at every transfer of a sector for data check. The output of a decoder 11 and the output of data of the head section of a sector of a register 14 correspond, and when the 2nd data are outputted from a decoder 11, the judgment machine 16

clears a counter 15 to 0, when the value of a timer 13 is 80 or less, but it is the case which is not so, and when the value of a counter 15 is less than eight, only 1 increases a value. A timer 13 is cleared by 0 with the next clock at this time.

[0020] That is, a timer 13 counts the number of clocks, and in advance of the data transfer of the head section of a sector, after 64 clock counts, if counting is carried out and enumerated data exceed 80 until it receives the data encryption data of the head of said sector, it will count up a counter 15 as time over.

[0021] Next, the actuation in the case of transmitting the data of 1 sector to the playback board 2 from drive 1 is explained in order according to the passage of time amount. It is placed between data transfer by CPU19. First, the data of 1 sector read to the buffer memory of the drive circuit 10, it is ending, and when CPU19 judges that there is an availability which receives the data of 1 sector in the buffer memory of the animation display circuit 18, the procedure of data transfer starts. CPU19 reads a random number from a random number generator 12, and inputs it into a random number generator 9 as initial value of a random number. Starting count-up of a timer 13 by read-out of the random number from a random number generator 12, a random number generator 12 performs renewal of a random number of 64 clock continuation from this time.

[0022] If initial value is inputted, a random number generator 9 will perform renewal of a random number of 64 clock continuation, and will output it to the

encryption machine 8. Since the data of the head of the sector from the drive circuit 10 are outputted to the encryption machine 8, the output of the encryption machine 8 brings the result of having enciphered the data of the head of the number of bits where 1 sector was appointed beforehand. CPU19 waits to complete renewal of a random number, reads the output of the encryption machine 8, and writes the data of this enciphered head in a decoder 11. Since read-out at this time is not original data transfer, the condition of the buffer memory of the drive circuit 10 does not change.

[0023] When encryption data are written in a decoder 11, count-up of a timer 13 stops. If excessive actuation has not been carried out to the interval when CPU19 transmits a random number to drive 1 from the playback board 2, and transmits encryption data to the playback board 2 from drive 1, the value of a timer 13 cannot be a not much bigger value than 64. Moreover, since the random number generator 9 and the random number generator 12 repeated the state transition only for the same number of steps from the same initial state at this time, the same random number should be outputted. Therefore, according to the output of a random number generator 12, a decoder 11 performs actuation that the encryption machine 8 is contrary to the actuation performed according to the output of a random number generator 9, and outputs the data of the head of 1 sector as the result. However, since this data is not original data transfer, it is

not outputted to the animation display circuit 18, but it is memorized only to a register 14.

[0024] Next, the data transfer for 1 sector containing the data of said head is started. According to the new random number which the random number generator 9 generated, it is enciphered with the encryption vessel 8, and the data of a sector are transmitted to a decoder 11 and restored by CPU19 according to the output of a random number generator 12. The data of the head of a sector and the output of a register 14 are collated, if the judgment machine 16 is not in agreement, it judges that the delivery side of data is not a Shinsei drive, counts up a counter 15, even if it is the case of being in agreement, also when the value of a timer 13 is 80 or more, judges that the random number generator by the side of delivery is an imitation as time over, and counts up a counter 15. Since a gate circuit stops outputting data when the value of a counter 15 is set to 8, playback is stopped. Of course, the value of the counter which makes playback stop may select integral values other than eight.

[0025] Finally, the main point in the case of applying this invention is explained. First, the shortest time amount taken to send a random number to a transmitting side from a receiving side, and to send encryption data to a receiving side from delivery and a transmitting side is found. The tolerance of a difference with the time amount which generating of the random number used for return from the

random number (it becomes the initial value of the random number generator 9 in a transmitting side) inputted in this and a transmitting side should take The count of the renewal of continuation of a random number is set up so that it may become below one half of the time amount which generating of a random number should take, and the number of clocks of the time delay which a judgment machine permits is set as 1.5 or less times of the number of clocks of renewal of continuation.

[0026] Although it is very difficult to operate its own circuit with the same clock frequency as Dedication IC when what is tried in order to reproduce the data reproduced unjustly tends to constitute a random number generator and an encryption machine combining commercial IC, it is comparatively easy to make it operate with the low clock frequency below one half. Moreover, if a limit of the response time is loose, it is also possible to perform count of a random number by software. Thus, unjust use will become easy if the time limit of a response is enlarged superfluously. In this invention, when the time amount which generation of a random number takes is severe to 1.5 or less times and the random number generator of dedication restricts the time amount which return of a random number takes, it has prevented that a receiving side is deceived by software, its own random number generator, etc.

[0027] The bus of PC system is a complicated transmission line where not an

object but the bus which operates at a different rate through a bridge is relayed, and data transfer between various kinds of equipments is not necessarily performed through an interface really. There are delay factors which change dynamically, such as interruption and memory refresh, among the delay factors as a transmission line besides a bridge or the static delay factor of an interface, and a response does not necessarily return in the aforementioned shortest time amount between the equipment of Shinsei. However, if a time limit is loosened in consideration of dispersion in a time delay, it will become weak to unjust use. In this invention, a response is not right, or when it is time over, and a counter is counted up and a counter reaches an upper limit, the method which interrupts a communication link is used, so that interruption of a communication link may not break out to the transmission error of time-out or data by the dynamic factor. If the probability for big delay to arise according to a dynamic factor is fully small and the upper limit of a counter is fully large, according to a dynamic factor, the probability for a communication link to be interrupted is seen from a practical viewpoint, and it can be considered that it is zero. On the other hand, since the time delay by limit of the working speed of its own random-number-generation means is a static delay factor, time-out occurs each time, a counter reaches a upper limit for a short time, and interruption of a communication link generates it certainly. It is important that initial value cannot be inputted into the random

number generator of a receiving side. If the input of initial value is possible, it will become possible to control so that the random number sent to a transmitting side becomes a specific value. Since the response to a specific initial value input becomes another specific value, it is easy to make the data which created the program which answers the another aforementioned specific value, deceived the receiving side, and were reproduced unjustly process. The input means of initial value should not be formed in the random number generator of a receiving side, but sufficient concealment should be given when preparing.

[0028]

[Effect of the Invention] As mentioned above, according to the digital data communication mode of this invention, it is possible to refuse processing of the data copied to another equipment from original equipment by judging a limit of the generating time amount of a random number and coincidence of the initial data of a sector for every transfer of a sector, and also when the secret about a code is broken especially, unjust use of data can be made very difficult from a limit of random-number-generation time amount.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The block block diagram showing the digital data communication mode in the gestalt of operation of this invention

[Drawing 2] The block block diagram in the data communication system of the conventional example

[Description of Notations]

1 23 Drive

2 24 Playback board

3 22 Bus

4 Five Bus interface

6 Seven Clock circuit

8 Encryption Machine

9 12 Random number generator

10 Drive Circuit

11 Decoder

13 Timer

14 Register

15 Counter

16 Judgment Machine

17 Gate Circuit

18 Animation Display Circuit

19 21 CPU

25 HDD

26 Bus Monitor Board

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－149022

(43)公開日　平成９年(1997)６月６日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/12			Ｈ０４Ｌ	9/00	６３１
Ｇ１１Ｂ	20/10		7736－5D	Ｇ１１Ｂ	20/10	Ｈ
// Ｇ０６Ｆ	1/00	３７０		Ｇ０６Ｆ	1/00	３７０Ｅ
	12/14	３２０			12/14	３２０Ｂ

審査請求　未請求　請求項の数２　ＯＬ　（全６頁）

(21)出願番号　特願平7－304122

(22)出願日　平成７年(1995)11月22日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　岡部　吉正
香川県高松市古新町８番地の１　松下寿電子工業株式会社内

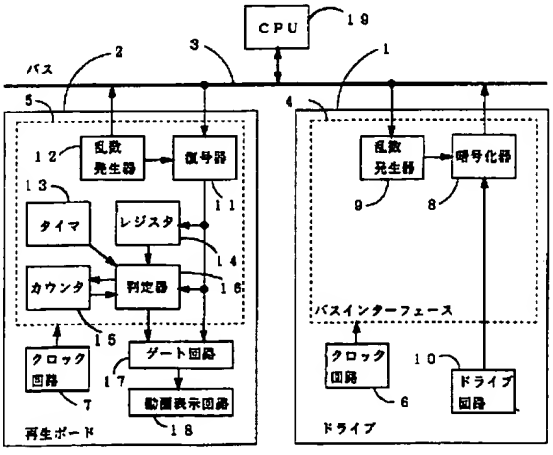
(74)代理人　弁理士　滝本　智之　（外１名）

(54)【発明の名称】　ディジタルデータ通信方式

(57)【要約】

【課題】　ＣＰＵバスに接続されるディスクドライブ装置と再生ボードを含むＰＣシステムにおいて、ディスクからのディジタルデータの不正使用を禁止し、著作権の保護を目的とする。

【解決手段】　ドライブ１と再生ボード２に同じ方式の乱数発生器９、１２を設け、再生ボード２から初期値としてドライブ１に乱数を転送し、ドライブ１からのセクターの先頭部データのみを暗号化した乱数を返送し、返送に要した時間に制限を設けると共に、次に前記先頭部データを含むセクターデータを転送し、先頭部データとの一致を判定器１６にて判定し、不正なデータの使用を禁止することにより、ＰＣ上での著作権のデータの複製使用を防止する。



1

【特許請求の範囲】

【請求項１】　回線を介して接続された第１の装置と第２の装置に、それぞれ初期値が定まるとその後は互いに同一の乱数を順次発生する第１の乱数発生装置と第２の乱数発生装置を配置し、ディジタルデータの送信に先立って、前記第２の乱数発生装置により発生された乱数を、前記回線を介して初期値として前記第１の乱数発生器に加え、その初期値に基づいて第１の乱数発生装置により発生された乱数により、送付すべきセクタデータの先頭値のデータを暗号化して前記第２の装置に送信し、続いてその送付すべきセクタデータの前記先頭部のデータを含むセクタデータを第１の乱数発生装置により順次発生される乱数により、暗号化して前記第２の装置に送信し、前記第２の装置においては、受信した前記の暗号化された先頭部のデータを前記第２の乱数発生装置により順次発生される乱数により復号化してレジスタに記憶し、続いて受信した前記先頭部のデータを含む暗号化されたセクタデータを前記第２の乱数発生装置の乱数により復号化し、その復号化されたセクタデータの先頭部データと前記のレジスタに記憶した先頭部データとの一致を判定し、不一致の回数が予め定められた回数に達すると第１の装置と第２の装置間の通信を遮断することを特徴とするディジタルデータ通信方式。

【請求項２】　第２の乱数発生装置が初期値を入力する手段を有せず、前記第２の乱数発生装置により発生された乱数を、前記回線を介して初期値として前記第１の乱数発生装置に送付してから、第１の装置から第２の装置に前記初期値を基に発生された乱数により暗号化されたセクタ先頭部データの暗号化データが返送されるまでに要した時間と、前記セクタ先頭部データの暗号化に用いる乱数の発生に要すべき時間との差の許容範囲を、前記乱数の発生に要すべき時間の半分以下に設定することを特徴とする請求項１記載のディジタルデータ通信方式。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ディジタル通信サービスの不正利用の防止に有効なディジタルデータ通信方式に関するものであり、特に著作権の設定されたディジタルデータの複製防止に有効なものである。

【０００２】

【従来の技術】近年の記録技術の発達によって、小型の光ディスクに数ギガバイトのデータを記録することが可能になり、画像圧縮の技術によって、前記の光ディスクに映画をディジタル記録することが可能になった。他方ではパーソナルコンピューター（以後、ＰＣと略す）の発達と普及により、前記の光ディスクに記録された映画をＰＣのモニタ上に再生する利用法が出現した。この利用形態では、光ディスクを読み取るドライブ装置（以後、ドライブと略す）と、圧縮記録されている画像データを伸張して表示する再生ボードを、ＰＣのバスに接続し、このバスを経由して画像データの転送を行うことになる。

2

【０００３】ディジタルコピーは複製によって画質が劣化しないので、ＰＣのデータの複製や変造に適した機能を利用し、ＰＣ内のハードディスクドライブ（以後、ＨＤＤと略す）や磁気テープに画像データをコピーすることが可能であり、他のＰＣにもコピー可能である。しかし、映画ソフトには著作権が設定されていて複製や変造が禁止されているので、ＰＣが持つ複製機能が有効に機能しないようにすることが必要となる。

【０００４】ＰＣで映画を再生する場合、画像データはバスを通して伝送されるので、複製防止の問題はバス型伝送路における盗聴防止問題に帰結する。バス型伝送路では受動的な傍受を検知して防止することは困難なので、傍受したデータが利用できない様にデータを暗号化する暗号通信を行うのが一般的であり、暗号通信を行う為には、送信側と受信側は鍵とよばれる秘密の情報を共有する必要がある。

【０００５】秘密の情報を要求する点ではパスワードシステムとも呼ばれる暗証番号方式と暗号方式は同じである。特開平２－６７０６７号公報は、暗証番号を要求して、返答された暗証番号が不一致であるか、もしくは一定時間内に返答がない場合に接続を拒否する方式を提案している。特開平３－１０９８５０号公報は試行錯誤によって偶然に正しい暗証番号が入力される確率を小さくするために、入力開始から一定時間経過した時点で、正しい桁数の正しい暗証番号が入力されているかどうかを、１回だけ検査する方式を提案している。どちらの特許も、時間の設定方法には詳しい説明を加えてないが、平均的な利用者が暗証番号を入力するのに要する時間の最大値に設定すると考えるのが合理的である。

【０００６】図２は従来例のブロック図であり、２１はＣＰＵ、２２はバス、２３はドライブ、２４は再生ボード、２５はＨＤＤ、２６はバス監視ボードである。この従来例の動作は、ＣＰＵ２１がソフトウエアに従ってバス２２を介してドライブ２３と再生ボード２４に鍵の入力と更新を行い、ドライブ２３は鍵を用いてデータを暗号化して送出し、再生ボード２４は鍵を用いてデータを復元するものである。この方式は、データをＨＤＤ２５にコピーし、後でＨＤＤ２５から再生ボード２４にデータを転送しようとしても、鍵を発生するソフトウエアが前回と全く同じ動作をしない限り、暗号化時に用いられた鍵を再生ボード２４に入力できないので正常な再生を行うことができない。しかし、ユーザーがバス監視ボード２６をバスに接続し、バス監視ボード２６は再生ボード２４への鍵の書き込みを検知して鍵を取り込み、データをＨＤＤ２５に記録する際に、前記バス監視ボード２６の取り込んだ鍵も記録しておくと、後でＨＤＤ２５から再生ボード２４にデータを転送する際に、暗号化時に用いられた鍵を再生ボード２４に与えられるので正常な

再生ができる。

【０００７】

【発明が解決しようとする課題】このようにＰＣで著作権の有する画像及び音声データによる映画等を再生するシステムにおいては暗号鍵を秘密にしなければならない。ＰＣ利用者はディスク上の映画等が記録された画像及び音声データを複製する権利は持たないが、ディスクに納められた画像及び音声データより映画等を再生する正当な権利を持っている。

【０００８】ドライブと再生ボードは同じ鍵を共有する必要があるので、何らかの手段を用いてドライブと再生ボードに鍵を入力する必要がある。出荷時に予め同じ鍵を入力し、以後は変更しない方式では、ドライブが出力したデータを一旦、ＨＤＤにコピーし、ＨＤＤから再生ボードに入力した場合でも、再生ボードにはドライブから直接入力されたデータと区別する手段がないので、通常の再生と同様に映画が再生される。ＨＤＤからの再生が可能であれば、ＨＤＤ上のデータをコピーした他のＰＣでも再生が可能なので、固定の鍵を用いる方式はコピー防止として有効でない。

【０００９】映画の再生中に鍵を更新する方式を用いた場合でも、ドライブと再生ボードの間の鍵の交換はＰＣ内で行われるので、ＰＣ内のデータの流れを監視することで鍵の入手が可能である。

【００１０】従って、有効なコピー防止を施す為には単にデータを暗号化するだけでは十分でなく、再生ボードに入力されたデータが、ドライブから直前に出力されたデータと同一であることを再生ボードが確認できる通信方式が必要である。また、最悪のケースとして暗号と鍵に関する秘密がＰＣ利用者に暴露された場合でも、再生ボードを騙すことが極めて困難である方式が望ましい。

【００１１】本発明は上記従来の問題点を解決するもので、鍵の更新手順を模倣された場合でも、鍵の更新に要する時間を検査して通信を拒絶し、ディジテルデータの複製防止を実現するディジタルデータ通信方式を提供することを目的とする。

【００１２】

【課題を解決するための手段】前記課題を解決するために、本発明のディジタルデータ通信方式は、回線を介して接続された第１の装置と第２の装置に、それぞれ初期値が定まるとその後は互いに同一の乱数を順次発生する第１の乱数発生装置と第２の乱数発生装置を配置し、ディジタルデータの送信に先立って、前記第２の乱数発生装置により発生された乱数を、前記回線を介して初期値として前記第１の乱数発生器に加え、その初期値に基づいて第１の乱数発生装置により発生された乱数により、送付すべきセクタデータの先頭値のデータを暗号化して前記第２の装置に送信し、続いてその送付すべきセクタデータの前記先頭部のデータを含むセクタデータを第１の乱数発生装置により順次発生される乱数により、暗号化して前記第２の装置に送信し、前記第２の装置においては、受信した前記の暗号化された先頭部のデータを前記第２の乱数発生装置により順次発生される乱数により復号化してレジスタに記憶し、続いて受信した前記先頭部のデータを含む暗号化されたセクタデータを前記第２の乱数発生装置の乱数により復号化し、その復号化されたセクタデータの先頭部データと前記のレジスタに記憶した先頭部データとの一致を判定し、不一致の回数が予め定められた回数に達すると第１の装置と第２の装置間の通信を遮断することを特徴としたものである。

【００１３】本発明によれば、送信すべきデータの一部を用いてデータの正当性を判定するとともに、データの再生に必要な暗号鍵を不正に得ることが非常に難しく、複製防止に有効である。

【００１４】

【発明の実施の形態】本発明の請求項１に記載のディジタル通信方式は、回線を介して接続された第１の装置と第２の装置に、それぞれ初期値が定まるとその後は互いに同一の乱数を順次発生する第１の乱数発生装置と第２の乱数発生装置を配置し、ディジタルデータの送信に先立って、前記第２の乱数発生装置により発生された乱数を、前記回線を介して初期値として前記第１の乱数発生器に加え、その初期値に基づいて第１の乱数発生装置により発生された乱数により、送付すべきセクタデータの先頭値のデータを暗号化して前記第２の装置に送信し、続いてその送付すべきセクタデータの前記先頭部のデータを含むセクタデータを第１の乱数発生装置により順次発生される乱数により、暗号化して前記第２の装置に送信し、前記第２の装置においては、受信した前記の暗号化された先頭部のデータを前記第２の乱数発生装置により順次発生される乱数により復号化してレジスタに記憶し、続いて受信した前記先頭部のデータを含む暗号化されたセクタデータを前記第２の乱数発生装置の乱数により復号化し、その復号化されたセクタデータの先頭部データと前記のレジスタに記憶した先頭部データとの一致を判定し、不一致の回数が予め定められた回数に達すると第１の装置と第２の装置間の通信を遮断することを特徴としたものであり、データの正当性を判定するために使用するデータは、送信データの一部であり、かつセクタデータ毎に判定しているため、正当なデータの判定の信頼性を増すことができる。

【００１５】次に請求項２に記載されたディジタルデータ通信方式は、第２の乱数発生装置が初期値を入力する手段を有せず、前記第２の乱数発生装置により発生された乱数を、前記回線を介して初期値として前記第１の乱数発生装置に送付してから、第１の装置から第２の装置に前記初期値を基に発生された乱数により暗号化されたセクタ先頭部データの暗号化データが返送されるまでに要した時間と、乱数の発生に要すべき時間との差から得る許容範囲を、前記セクタ先頭部データの暗号化に用い

る乱数の発生に要すべき時間の半分以下に設定することを特徴としたものであり、不当な複製を行うには２／３倍以上の高速なクロック周波数で乱数を発生する乱数発生器を用意しないと正常にデータの復号ができず、また、第２の乱数発生器は初期値入力手段を持たないので、初期値を偽造されることがなく、安全な乱数発生器が得られ、信頼性の高いデータの再生が出来る。　以下に、本発明の請求項１、及び請求項２に記載された発明の実施の形態について、図１を用いて説明する。図１において、１はドライブ、２は再生ボード、３はバス、４、５はバスインターフェース、６、７はクロック回路、８は暗号化器、９、１２は３２ビット長さの乱数発生器、１０はドライブ回路、１１は復号器、１３はタイマ、１４はレジスタ、１５はカウンタ、１６は判定器、１７はゲート回路、１８は動画表示回路、１９はＣＰＵである。

【００１６】以上の様に構成された映像再生システムの各部の動作を説明する。ドライブ１と再生ボード２はバス３に接続されている。バスインターフェース４、５はそれぞれクロック回路６、７が発生するクロックに同期して動作する。クロック回路６、７は同じ発振周波数で動作する。ドライブ側のバスインターフェース４は、暗号化器８と乱数発生器９とを持つ。暗号化器８は乱数発生器９が発生する乱数に従って、ドライブ回路１０から入力されるデータを暗号化してバス３に出力する。乱数発生器９は、バス３を介して入力された３２ビットの乱数を初期値として、初期値の入力後６４クロック間は１クロック毎に１回、それ以外の期間は暗号化器８が読み出される毎に１回の割合で出力する乱数を順次更新する。

【００１７】再生ボードのバスインターフェース５は、暗号化されたデータを復元する復号器１１と乱数発生器１２とタイマ１３と、レジスタ１４と、カウンタ１５と判定器１６を持つ。復号器１１は乱数発生器１２が発生する乱数に従って、バス３から書き込まれる暗号化データを元のデータに復元してレジスタ１４と判定器１６とゲート回路１７に出力する。ゲート回路１７は判定器１６から禁止信号が出ていない期間は復号器１１からの入力を動画表示回路１８にそのまま出力するが、禁止信号が出ている期間はデータを出力しない。

【００１８】ドライブ１から再生ボード２へのデータ転送はセクタと呼ばれる一定長のブロックを単位として行われる。前記乱数発生器１２は、ドライブ１側の乱数発生器９と同一発生方式のものであり、両者の初期値が一致すると以後は両者とも同じ乱数を順次発生する。また、乱数発生器１２は初期値を出力後、乱数発生器９と同期して、乱数の読出の６４クロック後までの期間は１クロック毎に１回、それ以外の期間は復号器１１にデータが書き込まれる毎に１回の割合いで乱数を更新する。但し、再生ボード２の乱数発生器１２はドライブ１の乱数発生器９と異なり、乱数の初期値を入力する手段を持たないので、特定の初期値から乱数を発生する様に外部から制御することはできない。タイマ１３は乱数発生器１２が初期値を読み出してから、復号器１１にドライブ１側より送られるセクタの先頭部のデータの暗号化されたデータが書き込まれるまでの時間を測定する。レジスタ１４は復号器１１が前記先頭部の暗号化されたデータ３２ビットを復号した結果を記憶する。先頭部のデータのビット数は３２ビットに限らず１６ビット、８ビットでもＰＣのバス幅を考慮して決めればよい。

【００１９】判定器１６は乱数発生器１２の乱数が読み出された時点からゲート回路１７に禁止信号を出力する。タイマ１３は乱数発生器１２が乱数を送り出し、ドライブ１側から先頭部のデータが返ってくるまでの時間を計測し、タイムオーバを監視し、カウンタ１５はタイマ１３のタイムオーバーと先頭部のデータの値の不一致時カウントアップし、カウンタ値が８未満の場合は、復号器１１が先頭部のデータを出力した時点の次のクロックでゲート回路１７への禁止信号の出力を停止するが、カウンタ１５の値が８の場合は、そのまま禁止信号の出力を続ける。乱数発生器の読み出し後の先頭の復号データはカウンタ１５の値によらず動画表示回路１８には出力されず、即ち、セクターの先頭部のデータはセクタの転送の度に一度データチェック用に用いられる。判定器１６は復号器１１から２番目のデータが出力された時点で、復号器１１の出力とレジスタ１４の出力が、セクターの先頭部のデータが一致し、かつ、タイマ１３の値が８０以下である場合にはカウンタ１５を０にクリアするが、そうでない場合であってカウンタ１５の値が８未満の場合は値を１だけ増やす。この時点の次のクロックでタイマ１３は０にクリアされる。

【００２０】即ち、タイマ１３はクロックの数をカウントし、セクターの先頭部のデータの転送に先立って、６４クロックカウント後、前記セクターの先頭のデータの暗号化データを受け取るまで計数し、計数値が８０を越えるとタイムオーバーとしてカウンタ１５をカウントアップする。

【００２１】次に、１セクタのデータをドライブ１から再生ボード２に転送する場合の動作を、時間の流れに従って順に説明する。データ転送にはＣＰＵ１９が介在する。まず、ドライブ回路１０のバッファメモリに１セクタのデータが読み出し済みであり、動画表示回路１８のバッファメモリに１セクタのデータを受け入れる空き容量があるとＣＰＵ１９が判断した時点でデータ転送の手順が始まる。ＣＰＵ１９は乱数発生器１２から乱数を読み出して乱数発生器９に乱数の初期値として入力する。乱数発生器１２からの乱数の読み出しでタイマ１３のカウントアップを開始し、乱数発生器１２はこの時点から６４クロック連続の乱数更新を行う。

【００２２】乱数発生器９は初期値が入力されると６４

クロック連続の乱数更新を行い、暗号化器８に出力する。暗号化器８にはドライブ回路１０からのセクターの先頭のデータが出力されているので、暗号化器８の出力は１セクタの予め定められたビット数の先頭のデータを暗号化した結果になる。ＣＰＵ１９は乱数の更新が終了するのを待って暗号化器８の出力を読み出し、この暗号化された先頭のデータを復号器１１に書き込む。この時の読み出しは本来のデータ転送ではないので、ドライブ回路１０のバッファメモリの状態は変化しない。

【００２３】復号器１１に暗号化データが書き込まれた時点でタイマ１３のカウントアップが停止する。ＣＰＵ１９が再生ボード２からドライブ１へ乱数を、ドライブ１から再生ボード２へ暗号化データを転送する合間に余分な動作をしていなければタイマ１３の値は６４より余り大きな値にはなっていないはずである。また、この時点で乱数発生器９と乱数発生器１２は同じ初期状態から同じステップ数だけ状態遷移を繰り返したので同じ乱数を出力しているはずである。従って復号器１１は乱数発生器１２の出力に従って、暗号化器８が乱数発生器９の出力に従って行った操作と逆の操作を行い、その結果として１セクタの先頭のデータを出力する。但しこのデータは本来のデータ転送ではないので動画表示回路１８には出力せず、レジスタ１４にだけ記憶する。

【００２４】次に、前記先頭のデータを含む１セクタ分のデータの転送を開始する。セクタのデータは乱数発生器９が発生した新たな乱数に従って暗号化器８により暗号化され、ＣＰＵ１９によって復号器１１に転送されて、乱数発生器１２の出力に従って復元される。判定器１６はセクタの先頭のデータとレジスタ１４の出力を照合し、一致しなければデータの送り側が真正なドライブでないと判断してカウンタ１５をカウントアップし、一致した場合であってもタイマ１３の値が８０以上の場合もタイムオーバーとして、送り側の乱数発生器が模造品であると判断してカウンタ１５をカウントアップする。カウンタ１５の値が８になるとゲート回路がデータを出力しなくなるので、再生はストップする。もちろん、再生をストップさせるカウンタの値は８以外の整数値を選定してもよい。

【００２５】最後に、本発明を適用する場合の要点を説明する。まず、受信側から送信側へ乱数を送り、送信側から受信側へと暗号化データを送るのに要する最短時間を求め、これと送信側において入力された乱数（送信側での乱数発生器９の初期値となる）から返送に用いる乱数の発生に要すべき時間との差の許容範囲を、乱数の発生に要すべき時間の半分以下になるように乱数の連続更新の回数を設定し、判定器が許容する遅延時間のクロック数を連続更新のクロック数の１．５倍以下に設定する。

【００２６】不正に複製したデータを再生しようと試みるものが、乱数発生器と暗号化器を市販のＩＣを組み合わせて構成しようとした場合、自作の回路を専用ＩＣと同じクロック周波数で動作させるのは極めて困難であるが、半分以下の低いクロック周波数で動作させることは比較的容易である。また、応答時間の制限が緩ければ、乱数の計算をソフトウエアで実行することも可能である。このように、応答の制限時間を不必要に大きくすると不正利用が容易になる。本発明では乱数の返送に要する時間を、専用の乱数発生器が乱数の生成に要する時間の１．５倍以下に厳しく制限することにより、ソフトウエアや自作の乱数発生器などによって受信側が騙されることを防止している。

【００２７】ＰＣシステムのバスは必ずしも一体物ではなく、ブリッジを介して異なる速度で動作するバスが中継され、インターフェースを介して各種の装置間のデータ転送が行なわれる複雑な伝送路である。伝送路としての遅延要因には、ブリッジやインターフェースといった静的な遅延要因の他に、割り込みやメモリリフレッシュといった動的に変化する遅延要因があり、真正の装置間でも必ずしも前記の最短時間内に応答が返るとは限らない。しかし、遅延時間のばらつきを考慮して時間制限を緩めると不正利用に対して弱くなる。本発明では、動的要因による時間切れやデータの伝送誤りに対しては通信の中断が起きないように、応答が正しくないかタイムオーバである場合にはカウンタをカウントアップし、カウンタが上限に達した時点で通信を中断する方式を用いる。動的要因によって大きな遅延が生じる確率が十分に小さく、カウンタの上限値が十分に大きければ、動的要因によって通信が中断する確率は実用的な観点から見てゼロと見なせる。一方、自作の乱数発生手段の動作速度の制限による遅延時間は静的な遅延要因なので、時間切れが毎回発生してカウンタは短時間で上限値に達し、確実に通信の中断が発生する。受信側の乱数発生器に初期値を入力できないことは重要である。もし、初期値の入力が可能であれば、送信側に送る乱数が特定の値になるように制御することが可能になる。特定の初期値入力に対する応答は別の特定の値になるので、前記の別の特定の値を応答するプログラムを作成して、受信側を騙して不正に複製したデータを処理させることは容易である。受信側の乱数発生器には初期値の入力手段を設けるべきではなく、もし設ける場合には十分な隠蔽を施すべきである。

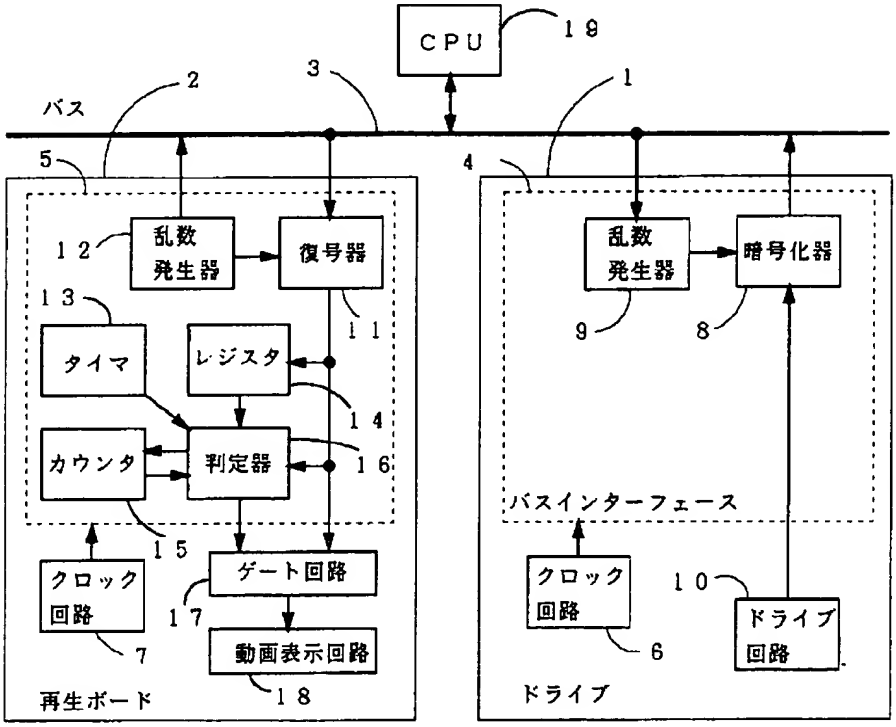
【００２８】

【発明の効果】以上のように、本発明のディジタルデータ通信方式によれば、乱数の発生時間の制限とセクターの先頭データの一致をセクターの転送毎に判定することにより、本来の装置から別の装置にコピーされたデータの処理を拒否することが可能であり、特に、暗号に関する秘密が破られた場合にも、乱数発生時間の制限からデータの不正利用を極めて困難にすることができる。

【図面の簡単な説明】

【図１】本発明の実施の形態におけるディジタルデータ通信方式を示すブロック構成図
【図２】従来例のデータ通信方式におけるブロック構成図
【符号の説明】
1、２３　ドライブ
2、２４　再生ボード
3、２２　バス
4、5　バスインターフェース
6、7　クロック回路
8　暗号化器
9、１２　乱数発生器
＊１０　ドライブ回路
１１　復号器
１３　タイマ
１４　レジスタ
１５　カウンタ
１６　判定器
１７　ゲート回路
１８　動画表示回路
１９、２１　ＣＰＵ
２５　ＨＤＤ
２６　バス監視ボード
＊

【図１】



【図２】